White Paper

Initiatives and Technologies

Intel's Ts Deliver New Platform Enhancements Beyond Gigahertz

R M Ramanathan
Technology Leadership Marketing
Intel Corporation

Introduction

In 2001, Intel's current CEO, Paul Otellini, detailed Intel's efforts in understanding the requirements of end users and delivering products to meet their needs. He spoke of "moving beyond gigahertz (GHz)" and expanding the company's focus on fundamental technologies and features for delivering greater value and functionality. Since that time, Intel has introduced products that deliver on this commitment, including Hyper-Threading Technology,[1] Intel® Centrino® mobile technology,[+] and the Intel® 915 G/P, 925X Express Chipsets, iCafé platforms, and platforms for digital home, digital office, and more.

Today in 2005, Intel has realigned itself as a platforms company, and our definition of "platform" goes beyond performance and even capabilities. It includes conducting people-focused research to determine what users need and desire then leading the industry in delivering those capabilities and experiences.

One group of technologies Intel has specifically designed to deliver these capabilities on the platform is referred to by Intel as the "*Ts," or "star Ts" (advanced technologies). A premier collection of technologies embedded into microprocessor, platform silicon and software, the Ts represent an evolution in the way computer platforms are designed and used. Intel's combination of user-focused research and development (R&D), ability to drive Moore's Law, manufacturing strength and our ecosystem-enabling efforts allow us to design and introduce these new capabilities to users worldwide.

With the Ts, Intel is able to deliver end user benefits to platforms in all segments, providing features that enhance security, multi-tasking, mobility, manageability, reliability, flexibility, performance, and more. To put more resources in these directions, Intel has realigned its strategy and moved resources away from pure performance-oriented projects to developing platforms that delivers the new level of end user experience.

1. Hyper-Threading Technology (HT Technology): Using HT Technology with this product requires a Pentium 4 processor that supports this feature and an HT Technology-enabled chipset, BIOS and operating system. See **http://support.intel.com/support/motherboards/server** for more information, including details on which processors and operating systems support this feature.

A Natural Extension of Moore's Law

Coined in 1965, Moore's Law has accurately predicted the doubling of the number of transistors in an integrated circuit every couple of years. Intel has recognized that with the ever-increasing number of transistors also comes ever-increasing opportunities to add more innovations and capabilities to microprocessors and platform silicon. A good example is Intel® Centrino® mobile technology, which combines communications, power management, chipset and processor capabilities into a single silicon platform (see Figure 1).

Today, as people see value in performance gains beyond simply speeding up applications, Intel sees opportunities for the seamless integration of end user features across a wide variety of computing platforms. Through the Ts, Intel can deliver new user-focused platforms for the digital home, digital office, enterprise and mobility markets that are optimized to do everything from download movies from the Internet faster to effortlessly run more than one operating system (OS) simultaneously on the same computer.

Examples of other benefits include hardware-based security features, multi-threading (the ability to run multiple processor-intensive applications concurrently), enabling a processor to access larger amounts of memory than 32-bit code supports, and the ability to remotely access networked clients even when they are turned off, or lack a working operating system or functional hard drive.

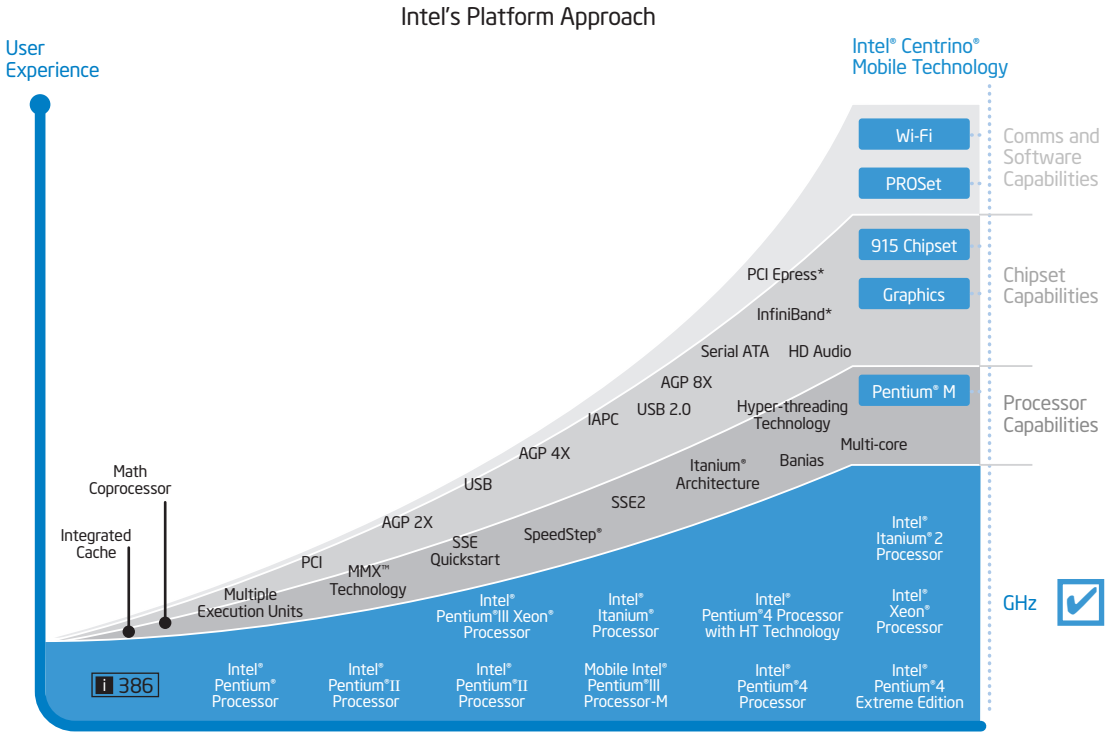


Figure 1: Intel takes advantage of Moore's Law through Intel's platform approach—putting more capabilities on the platform. Intel® Centrino® mobile technology is a prime example.

How We Develop the Ts

Intel's world-class team of researchers continually delivers breakthrough technologies to the industry. Translating research into products is one of Intel's greatest strengths. Through Intel's extensive R&D, platform- and ecosystem-enabling capabilities, we are delivering compelling new features to the marketplace, which are accelerating disruptive industry shifts like the Internet, wireless, and broadband technologies.

During every phase of the development path to a T, we try to involve customers and users through a number of methods. One method is through **ethnographic research** into how people use or potentially would use technology, either existing or proposed, in their daily lives. We develop repeatable processes to take new ideas from research through technology readiness to product.

We also look to our customers and ecosystem co-travelers to provide us input on how to improve our products from generation to generation. We've conducted studies with IT managers, original equipment manufacturers (OEMs), independent software vendors (ISVs) and others in the industry on how computing uses will evolve, and many other areas.

A Look at Where the Ts Are Today

Here's a quick list of the current technologies that comprise the Ts:

- Hyper-Threading Technology
- Intel® Virtualization Technology
- Intel® Extended Memory 64 Technology
- Intel® Active Management Technology
- LaGrande (Intel codename) Technology
- Intel® I/O Acceleration Technology

The Ts that are shipping in volume Intel® platforms today include Hyper-Threading Technology in numerous platforms, and Intel Extended Memory 64 Technology in enterprise/server platforms. Other Ts will deploy on various platforms over the next two to three years. What follows is a brief description of each of these Ts.

Hyper-Threading Technology

Introduced in 2002, this technology enables one physical processor to appear and behave as two virtual processors to the operating system. For consumers and businesses of all sizes, (HT Technology) offers more efficient multitasking and system responsiveness. Users enjoy improved performance running multiple applications simultaneously, such as running a virus scan or encoding video in the background while playing a game. For IT managers, HT Technology means more efficient use of processor resources, greater throughput, and improved performance.

HT Technology's key advantage is that it allocates and reallocates processor resources to applications as they need horsepower. By enabling multi-threaded software applications to execute threads in parallel, HT Technology maximizes the efficiency of the processor by allowing it to complete more tasks in a given amount of time.

HT Technology is a precursor to dual-core and multi-core processors due in the coming years. In the last two years, Intel has shipped more than 50 million desktop, mobile, and server processors with HT Technology.

Intel® Virtualization Technology

Virtualization enables a system to run different programs and even entire operating systems on the same machine at the same time. Intel Virtualization Technology takes virtualization a step further by providing hardware and platform support that makes virtualization more seamless and secure. Partitioning a system for multiple uses, Intel Virtualization Technology enables one hardware platform to function as multiple "virtual" platforms (see Figure 2). In the home, for instance, Intel Virtualization Technology could enable one family member to be in a room using a PC for gaming while a family member in another room uses a mobile device to simultaneously use the same PC for photo-editing.

For businesses, Intel Virtualization Technology offers many advantages, including improving manageability, limiting downtime and maintaining worker productivity. For example, an IT staff could perform a number of remote operations on networked clients while not disrupting a single worker. By helping to improve the resilience and reliability of the platform through virtualization, it offers greater reliability, efficiency and flexibility for server consolidation, legacy migration and security.

Intel Virtualization Technology combined with appropriate software can enable greater reliability and performance for both enterprise and consumer uses. By enabling multiple, independent software environments (partitions) inside a single system, operations in one partition won't impact operations in the other partitions. What's more, by moving some of the arbitration into hardware, the technology offers several key advantages over software-only virtualization solutions. It reduces the software overhead, plus increases the performance and robustness of the entire solution by enabling the virtualized partitions to have more efficient access to system hardware.

Intel® Extended Memory 64 Technology

Introduced in 2004 for workstations and high-performance computer server platforms, **Intel® Extended Memory 64 Technology** (Intel® EM64T) allows server, workstation, and desktop platforms to access larger amounts of memory. This enhancement allows a processor to run newly written 64-bit code and access larger amounts of memory than 32-bit code. With appropriate Intel EM64T-supporting hardware and software, Intel EM64T-based platforms can enable use of both extended virtual and physical memory.

Desktop introduction of the technology is planned in 2005 along with the release of the Microsoft Windows XP Professional x64* operating system. Intel is providing tools, technical support and expertise for those vendors optimizing their solutions for Intel EM64T and other Intel platform capabilities.

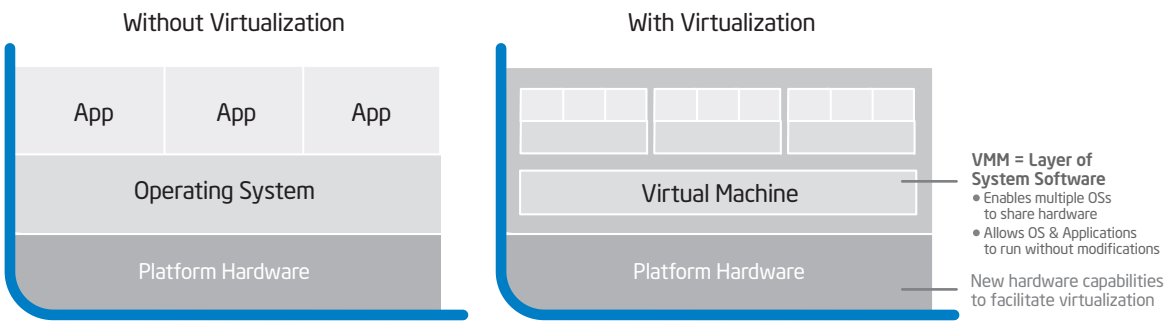


Figure 2: Intel Virtualization Technology adds a set of hardware enhancements to the platform so that one platform functions as multiple "virtual" platforms.

Intel® Active Management Technology

Intel's latest addition to the Ts, **Intel® Active Management Technology** (Intel® AMT), promises to make life easier for IT managers and businesses of all types. The technology enables IT managers to remotely access every networked computing system—even those that lack a working operating system or hard drive, or are turned off.

Intel AMT was designed in response to problems specifically identified by IT organizations and is a significant step in Intel's vision for the **digital office** initiative. This initiative is targeted to provide such sought-after features as proactive management, system availability, malware protection, and information security. Intel AMT is one of several capabilities Intel is delivering within this initiative as "embedded IT."

Intel AMT provides solutions for three of the most pressing issues identified by today's IT managers: reducing desk-side visits, improving asset management, and reducing downtime. By using nonvolatile memory to store information, Intel AMT provides tamper-resistant troubleshooting, recovery, and inventory management capabilities that are accessible whether the operating system is running or not. Its integration into hardware and firmware helps prevent intentional or accidental tampering. Intel AMT even allows storage of security agents so systems can remain better protected even if the hard drive fails or the operating system becomes inoperable.

With Intel AMT, IT managers can more easily remotely monitor and maintain networked computing platforms for various issues, viruses, security vulnerabilities, and inventory accounting while maintaining user privacy and choice (see Figure 3). Intel AMT will also help reduce total cost of ownership (TCO) by enabling IT personnel to focus more of their time on transforming the business through other IT investments. Intel AMT is expected to be available in 2005 on Intel platforms.

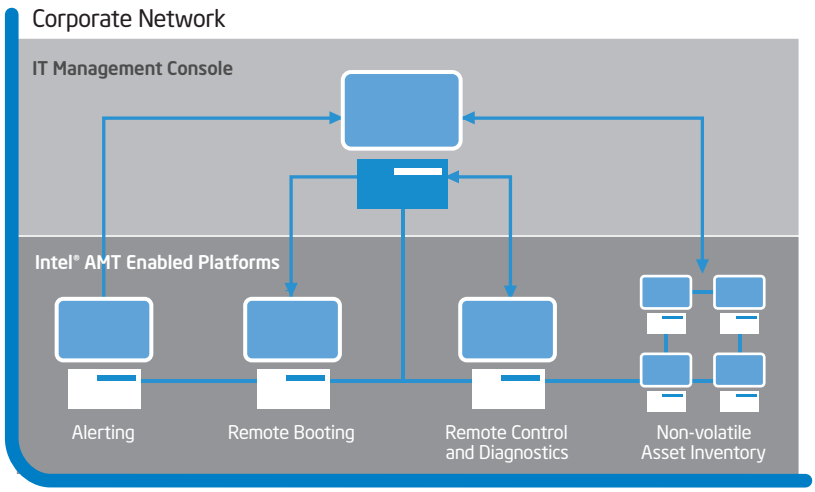


Figure 3: With Intel® AMT out-of-band (OOB) system management capabilities, IT can remotely manage PCs regardless of system power or OS state.

LaGrande Technology

Today's users want secure systems. While a 100 percent secure computing world is probably next to impossible, **LaGrande Technology** (LT) brings a new level of protection. By enabling protected execution, protected input/output (I/O), and sealed storage, LT provides a solid hardware foundation that helps protect sensitive information from software-based attacks without compromising usability.

LT is a versatile set of client hardware enhancements to Intel® processors, chipsets, and platforms that help protect the confidentiality and integrity of data stored or created on the client PC. LT-enabled platforms provide a sound hardware foundation for strengthening operating systems and applications—and affording users additional peace of mind.

LT will be available on desktop platforms with the release of "Longhorn" operating system. Microsoft's Next Generation Secure Computing Base (NGSCB) will build upon capabilities enabled by LT.

Intel® I/O Acceleration Technology

Network bandwidth is exponentially increasing in corporate networks, from Fast Ethernet to Gigabit Ethernet (GbE) and now 10-Gigabit Ethernet (10 GbE). Throughout this evolution, network server performance has kept pace with network traffic increases—until recently. Increasingly, network traffic demands are outpacing the ability of servers to keep up, and the gap continues to widen with ever-increasing network communications and transaction processing workloads.

Intel® I/O Acceleration Technology (Intel® I/OAT) is a server platform network I/O accelerator that takes a platform approach to addressing this traffic problem by breaking up the data-handling job among all of the components that make up the platform—the processor, chipset, network controller, and software. This distribution approach reduces the workload on the processor while accelerating the flow of data. The processor's job is reduced by giving the chipset and network controller responsibility for moving data in and out of memory. Intel also optimized the TCP/IP protocol—an open "etiquette" that enables all types of computers to exchange data via a common language—for Intel®-based servers, which cuts the processor's workload in half, further freeing it to work on other jobs. Highlights of Intel I/OAT are shown in Figure 4.

"Intel I/OAT demonstrates the advancements that are possible when a problem is approached from a platform perspective," said Pat Gelsinger, senior vice president, Intel Digital Enterprise Group. "The benefit to end users is better performance, particularly on transaction applications, such as Web commerce or electronic banking, while businesses benefit from reduced cost of ownership and improved ability to grow the system."

Microsoft plans native support for Intel I/OAT in upcoming releases of Windows Server.

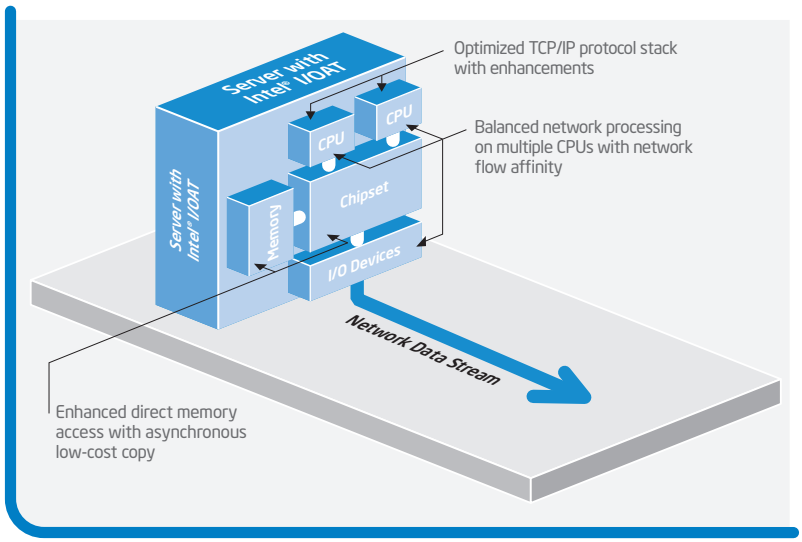
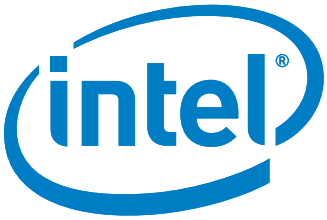


Figure 4: Intel® I/OATs system-wide network I/O acceleration technologies.



www.intel.com

More Platform Features, More Capabilities

The variety of ways people use computing and communications devices continues to evolve, as do the devices themselves. Speed will increasingly become just one part of performance. Consequently, Intel will pursue further development of threading technologies and new processors incorporating HT Technology, dual-core and multi-core designs.

Intel will also continue to investigate new capabilities and end user benefits that can be designed into Intel silicon and integrated across computing platforms. Areas that Intel is broadly researching include optimizing 3D and animated graphics, data mining, network processing, speech recognition, and synthesis.

Summary

As the range of uses for computing and communications devices grows, Intel has recognized sheer GHz speed as only one component of performance. The company is leveraging our user-focused research and development, ability to drive Moore's Law, manufacturing strength and our ecosystem-enabling efforts in new ways to bring value-added features and capabilities to client devices through key platform silicon technologies like the Ts.

Embedded into microprocessor and platform silicon, this collection of technologies represents an evolution in the way computer platforms are designed and used. With the Ts, people can expect to see end user benefits to platforms in all segments, including features that enhance security, multitasking, mobility, manageability, reliability, flexibility, performance, and more.

More Info

You can learn more about these integrated technologies at the Intel Web site:

- Hyper-Threading Technology
- Intel® Active Management Technology
- Intel® Extended Memory 64 Technology
- Intel® I/O Acceleration Technology
- Intel® Virtualization Technology
- LaGrande Technology

Author Bio

R.M. Ramanathan has been a technology evangelist in Sales and Marketing Group for the past two years. In his 10 years with Intel he has held various positions, from engineering to management. Before coming to Intel, Ramanathan was director of engineering for a multinational company in India. He has received four patents and has 10 patents pending in the areas of networking and security. Ramanathan holds a master's degree in mathematics from Madurai Kamaraj University in India.

+ Wireless connectivity and some features may require you to purchase additional software, services or external hardware. Availability of public wireless LAN access points is limited and some hotspots may not support Linux*-based Intel Centrino mobile technology systems. System performance measured by MobileMark* 2002. System performance, battery life, wireless performance and functionality will vary depending on your specific operating system, hardware and software configurations. See **www.intel.com/products/centrino/more_info** for more information.

Printed in the United States. 0105/XXX/HBD/XX/PDF 309161-XXXUS